SYSTEM AND METHOD FOR VERIFYING COMPUTER PROGRAM CORRECTNESS AND PROVIDING RECOVERABLE EXECUTION TRACE INFORMATION

ABSTRACT OF THE DISCLOSURE

In a system for statically analyzing a specified computer, a verification condition generator converts the program into a logical equation, called a verification condition, and inserts program flow control labels into the sub-equations of the verification condition. The flow control labels identify conditional branch points in the specified computer program. A theorem prover is applied to the logical equation to determine truth of the logical equation, and when the truth of the logical equation cannot be proved, the theorem prover generates at least one counter-example identifying one of the conditions, one or more variable values inconsistent with that condition, and any of the flow control labels for conditional branch points of the program associated with the identified variable values. A post processing module converts each counter-example into an error message that includes a program trace when the counter-example identifies one or more of the flow control labels.